NewStatesman

Spotlight

CYBER SECURITY: PROTECTING PEOPLE ONLINE

Brad Smith / Dr Jessica Barker / Brandon Lewis

Even tech experts are only human

One Thursday in early December 2018, some 32 million mobile users in the United Kingdom were faced with a 21st century existential nightmare: for hours they were unable to make calls, send texts or use the 4G network. The outage affected people signed up to O2, Giffgaff and other operators using the Telefonica network. The effects were so widespread that, as far afield as Japan, mobile users lost smartphone coverage for a full five hours.

The culprit was not some sophisticated cyber ware or malicious hack, however. As the day unfolded, the issue turned out to have been perhaps the most obvious plot-twist to the story: human oversight. The root of the mega-outage was an expired digital certificate in a management software by Ericsson, the Swedish telecommunications firm. This was not the first time the company was blamed for a smartphone blackout. In 2012, O2 said an outage that also affected millions of customers was down to a fault in central user database provided by Ericsson.

Not only do such incidents cause a major headache for mobile users, but a mistake like letting a certificate expire can leave firms vulnerable to hackers, cyberattacks and further breaches. No organisation operating today can afford to be complacent about cyber security. According to the Cyber Security Breaches Survey 2019, released in April, some 27 per cent of UK business and charities had experienced a cyberattack in the past 12 months, down from 43 per cent the previous year.

Human fallibility is at the heart of many such incidents, with hackers exploiting over-worked employees on the receiving end of a daily barrage of emails. That same poll found that of UK cyberattacks, 80 per cent were phishing-related, and almost a third involved hackers impersonating senior management via email. Research by Kroll, a risk solutions provider, found that 88 per cent of UK data breaches last year were the result of human error. Meanwhile, a poll by US software company Centrify found that 77 per cent of UK workers have no basic training in cyber security.

But, as the 2018 outage shows, the most sophisticated technology is vulnerable to the shortcomings of those who use it. Tech can't innovate human error out of existence. Alongside technological security solutions, employers need to support staff in recognising when they might be vulnerable to malicious intent. And to make sure they renew that digital certificate.

NewStatesman
Standard House
12-13 Essex Street
London, WC2R 3AA
Subscription inquiries:
digital.subscriptions@
newstatesman.co.uk

Account Managers
Jugal Lalsodagar
Dominic Rae
Cyrus Ramezani

Commercial Director
Peter Coombs

Special Projects Editor
Alona Ferber

Special Projects Writers
Jonny Ball
Rohan Banerjee

Design and Production
Leon Parks

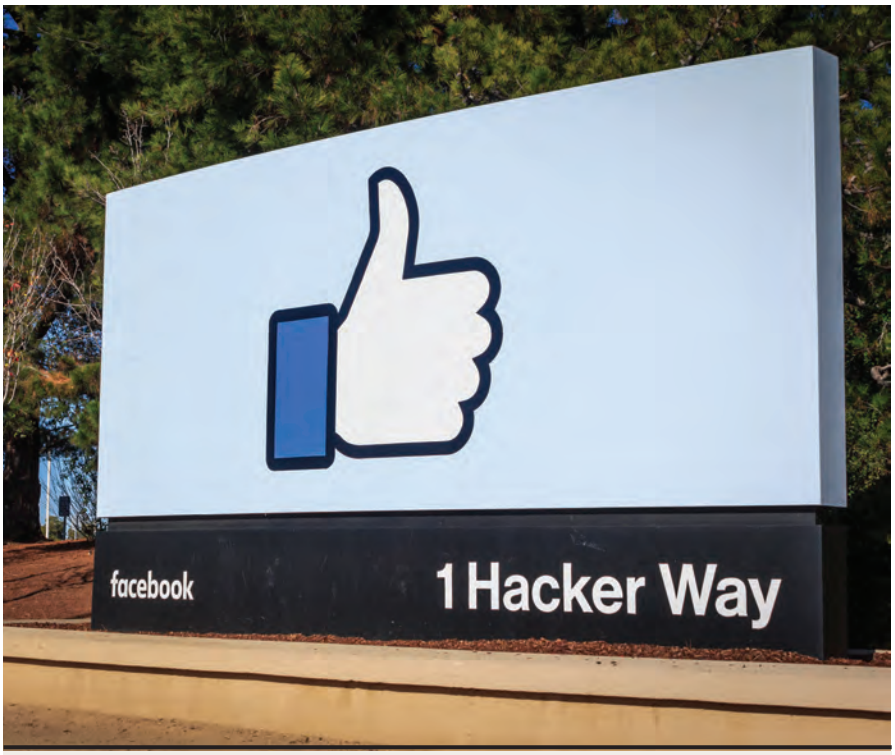
Cover illustration
Sam Falconer

BRITISH SOCIETY OF MAGAZINE EDITORS AWARDS 2017 WINNER

First published as a supplement to the *New Statesman* of 1st November 2019. Registered as a newspaper in the UK and US. The paper in this magazine is sourced from sustainable forests, responsibly managed to strict environmental, social and economic standards. The manufacturing mills have both FSC and PEFC certification and also ISO9001 and ISO14001 accreditation.

This supplement can be downloaded from: newstatesman.com/page/supplements

News



SHUTTERSTOCK/ ACHINTHAMB

Facebook expands bug bounty scheme

Rohan Banerjee

Facebook has revamped its bug bounty programme, broadening the eligibility criteria of the types of vulnerabilities it will pay out for. The company is stepping up efforts to stop the exploitation of user data collected via third-party applications and services hosted on its site.

Facebook began paying bounties in 2018 for certain bugs that security researchers might find in apps that integrated with its own hardware or software. This latest move, Facebook's security engineering manager Dan Gurfinkel explained in a statement, is designed to encourage more vigilance from app developers as to how their technology or data streams could be abused by "actively engaging with the wider cyber security ecosystem".

If ethical hackers, with the authorisation of the developer in question, are able to demonstrate a weakness within an app hosted by Facebook, they can claim a cash reward. Facebook offers a minimum payout of $500 for qualifying bugs. There are bonuses of between $1,000-$15,000, meanwhile, for anyone able to find a problem in the code of Facebook's native products such as Messenger, Portal or Whatsapp.

Oxfordshire-based cyber firm in £3.1bn takeover

Samuel Kerr

A major British cyber security firm is to be sold for £3.1bn to Thoma Bravo, an American private equity group. Sophos, which boasts over 400,000 clients including Pixar, Toshiba and Ford, made headlines in 2017 for assisting the NHS following the WannaCry ransomware attack. The encryption and antivirus specialist is based in Abingdon, Oxfordshire and employs over 3,000 people worldwide. Its growth in recent years is attributed to the scalable nature of its security programmes, making them attractive to small businesses.

This acquisition comes as UK companies and sterling-denominated assets become increasingly attractive to overseas firms, with the value of sterling declining this year by almost a fifth since the EU referendum. Thoma Bravo is continuing its expansion into the cyber market, having already acquired stakes in McAfee and Barracuda Networks.

UK workers lack basic cyber skills

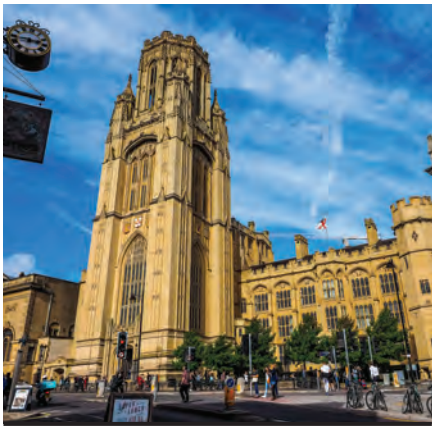
Rohan Banerjee

Over three quarters – 77 per cent – of people working in the United Kingdom have never been provided with basic cyber security training by their employers, a recent study has found. Centrify, an American software company, surveyed 2,000 full-time UK professionals across the public and private sectors.

The majority – 69 per cent – of respondents in Centrify's research said that they lacked confidence in their ability to keep their own or their

employer's digital information safe. Indeed, 27 per cent admitted to using the same login credentials across multiple accounts. And 14 per cent of those surveyed said that they kept unsecured paper copies of their passwords near or on their office desk.

Andy Heather, Centrify's vice-president, commented: "It is astounding to hear that so many UK companies neglect to instil even the most basic cyber security measures in their employees." He warned: "Just one misplaced password could result in the theft and abuse of millions of sensitive company documents."



SHUTTERSTOCK CLAUDIO DIVIZIA

Bristol and Bath launch cyber centre

Rohan Banerjee

The University of Bristol and the University of Bath have launched the United Kingdom's first Centre for Doctoral Training in Cyber Security after receiving funding from the Engineering and Physical Sciences Research Council (EPSRC).

A range of four-year PhD programmes, supervised by academics from both institutions, are available. These cover smart cities and digital infrastructure, wireless sensor technologies, cyber security in the manufacturing sector, and data science. In addition to students' theses, the courses involve a series of taught modules, relating to both the technical and human or social aspects of trust, identity, privacy and security (TIPS) issues at scale, and work placements within partner companies.

Awais Rashid, professor of cyber security at the University of Bristol and the centre's director, said that students would be given the skills required to thrive in a "hyper-connected future". He added: "Cyberattacks form one of the major threats to national and international security. We need future leaders in academia and industry who are able to anticipate the myriad trust, identity, privacy and security challenges in complex infrastructures and develop solutions to overcome them."

Government backs £36m security chip research

Rohan Banerjee

The business secretary, Andrea Leadsom, has committed £36m of government funding to a research project into the development of cyber security chips, led by the artificial intelligence firm Arm.

The chips are additive hardware that make it more difficult for hackers to breach and gain control of computer systems. "Cyberattacks can have a particularly nasty impact on businesses, from costing them thousands of pounds in essential revenue as well as reputational harm," Leadsom said in a statement.

The government is also supporting the Secure Wireless Agile Networks (SWAN) programme run between Toshiba Research Europe, the University of Bristol and GCHQ. SWAN aims to deliver more cyber-resilient public WiFi. The partners are developing new types of firewalls, while researching how to make systems more resistant to signal jamming. Leadsom explained: "Investing in our world-leading researchers makes good business and security sense."

SHUTTERSTOCK/MICHAELJUNG

Number of girls applying for NCSC courses soars

Samuel Kerr

The number of applications from girls for summer courses run by the National Cyber Security Centre has jumped by 47 per cent per cent since 2018. The rate of overall applications across all genders, meanwhile, has risen by 29 per cent.

NCSC, the dedicated digital security arm of GCHQ, organises courses lasting between one and five days for 11 to 17-year-olds. Programmes aim to develop young people's interest in computing and technology, and include lectures from guest speakers and practical exercises. Courses are held in Belfast, Cardiff, Paisley, Newcastle, Birmingham and London.

As women make up less than a quarter of the global cyber security workforce, the government is keen to diversify the UK's recruitment in this sector, encouraging more girls to participate in science, technology, engineering and mathematics (STEM) subjects. A recent poll from the Institute of Coding found that many young people in the UK are deterred from working in the digital sector, with the majority of respondents arguing that the industry needs to be more inclusive.

The president of Microsoft tells Oscar Williams about his new book on the digital world's most pressing challenges

Brad Smith's big idea

In December 2013, a select group of Silicon Valley leaders visited the White House. Facebook's Sheryl Sandberg, Google's Eric Schmidt and Microsoft's Brad Smith were among former president Barack Obama's guests. But this wasn't a celebration of the tech industry; the executives were there because two of the companies – Google and Microsoft – were suing the United States government.

Edward Snowden's revelations, published five months earlier, had sent a shockwave through the industry. The former National Security Agency contractor's cache of top secret documents revealed that the US had been spying on users of the world's biggest tech platforms. The scale of the surveillance was unprecedented, and the industry was meeting with Obama to push for change. But as the conversation in the Roosevelt Room unfolded, the president issued a warning to his guests. He noted that the US government had much less data than the companies they represented. "I have a suspicion," he said, "that the guns will turn." Nearly five years later, they have.

Last March it emerged that Cambridge Analytica, a British consultancy firm that worked on Donald Trump's presidential campaign, had acquired the data of tens of millions of Facebook users from a university researcher, in order to combine psychological profiling with political advertising.

According to Brad Smith, the president and chief legal officer of Microsoft – who recounts his meeting at the White House in a recently published book – the Cambridge Analytica scandal and the Snowden revelations represent "the two big technology inflection points in this decade".

Sitting in a clinically minimalist boardroom above Microsoft's Oxford Circus store, Smith refuses to be drawn on whether he now thinks Snowden is a hero or a traitor. "In the eyes of some," Smith writes in the book, "he was both." He is less equivocal, however, about the executives behind Cambridge Analytica. "No one's going to argue that Cambridge Analytica was good or that the people who ran it were heroes of our time," he says. "But in a sense [it] did a service of finally grabbing people's attention and causing government officials and legislators to focus more on privacy issues, in the United States in particular.… I think the real question in both [cases] is what the world does with what it learned."

GETTYIMAGES

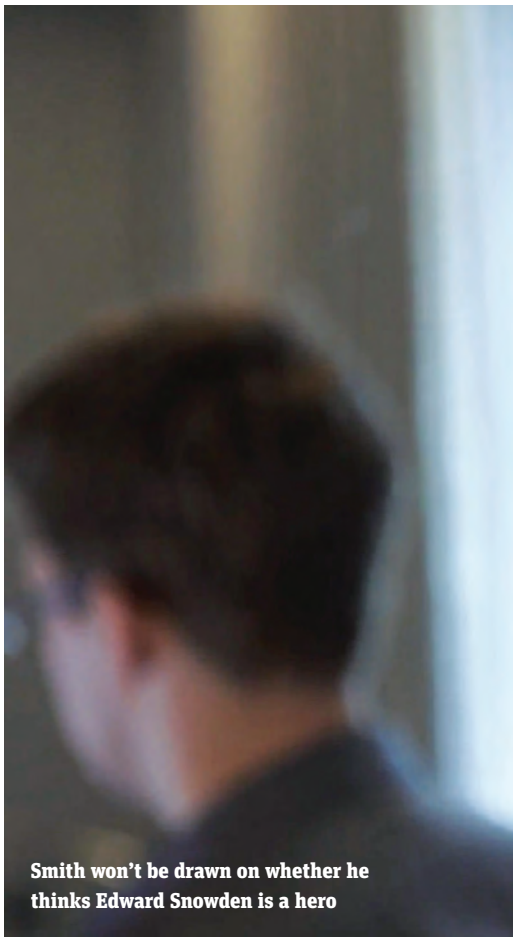
"It's too early to say if we'll need more regulation"

In recent years Smith has become one of the technology industry's most high-profile commentators. He has criticised his company's rivals for their use of data, called for new laws governing facial recognition, and laid the groundwork for a "Digital Geneva Convention" to set the parameters of cyber warfare. *Tools and Weapons: The Promise and The Peril of the Digital Age* – his first book – is a treatise on the modern technology industry's most pressing challenges.

As Smith's publishers prepared to go to print over the summer, a number of US politicians and agencies were paving the way for antitrust investigations into Silicon Valley's biggest companies. Microsoft, with years of antitrust battles under its belt, was exempt.

Smith was hired by Bill Gates to be Microsoft's general counsel in 2002 and spent a decade and a half fighting the antitrust fight. In an interview with the *Washington Post* in September, the veteran lawyer admitted that Microsoft "made more than [its] share of mistakes in the antitrust era, and I was personally responsible for almost all of them, to some degree." But today, some 17 years after Smith joined the company, Microsoft's reputation has been reformed. With a trillion dollar market cap, at the time of writing it is the world's most valuable company.

With the antitrust era behind him, Smith is broadening his focus to the industry as a whole and wants to solve one of its biggest challenges: the use of data. In *Tools and Weapons*, he and his co-writer, Microsoft communications director Carol Ann Browne, call for a new model for data sharing in the wake of the Snowden revelations and Cambridge Analytica scandal. It transfers the concentration of data from a small number of tech companies to shared trusts that are accessible to a network of organisations. "We need to do for data what open source did for code," he says. "It might be economically sensible for [car manufacturers] to federate certain aspects of their data because the alternative would be just to rely on the data moving to a single tech company.… [Manufacturers] that federate data are much more likely to retain the economic value for themselves and that's going to lead to a healthier automobile sector."



Smith won't be drawn on whether he thinks Edward Snowden is a hero

Proposing a model which increases data sharing might seem a counterintuitive way to respond to a string of privacy scandals. But advocates of data trusts argue that they increase competition, giving users and customers greater choice if an organisation fails to take their privacy seriously.

While Smith is a vocal champion of data trusts, he acknowledges that any plan to democratise access to data will inevitably pose its own security risks. "If data is federated and accessible by more than one organisation, the cyber security challenges of recent years take on an added dimension," he writes.

GETTY IMAGES

The book calls for developers to use tools that protect privacy and de-identify personal data.

Smith compares companies' current thirst for data to the gold rush. Two groups, he notes, made money in that era: "[There were] the people who found the gold and the people who produced the tools for the gold miners." Microsoft, says Smith, is "in the business of providing tools so that there can be gold-miners". With a smile, he adds: "Turn every automobile company into the miner of its own gold and do that in every sector of the economy."

In *Tools and Weapons*, Smith warns that if we continue along the current path, tech companies in the US and China will accumulate ever more data and power. In a future increasingly shaped by artificial intelligence, some commentators have speculated that these two countries' technological supremacy will present a major threat not just to other nations' security, but also their sovereignty.

Since Satya Nadella took over as chief executive of Microsoft five years ago, the company has shifted its focus from desktop software to cloud computing. Smith's vision plays to Microsoft's current strengths and may hurt rivals which are more dependent on advertising revenues. But Smith makes a plea for policymakers and business leaders to assess his ideas on their merits. "Let's not go to the ad-hominem attack until we first think about the idea because maybe it's a good one," he says.

"The second thing I would say is Microsoft is a very diversified technology company. It is true that advertising is a relatively small part of our business; it is also true that we have a digital advertising business of some real significance." Microsoft owns the professional social network LinkedIn, which, as Smith notes, has more users than Twitter. Its search engine, Bing, is also funded by advertising.

In Smith's vision, governments play two key roles. "If they do a better job of making data available publicly, then they start to level the playing field, because smaller players can combine their own data with publicly available data," he says.

The second role may prove less popular among Microsoft's competitors. "The government can even decide that it doesn't want to see the public data aggregated in a manner that would facilitate the use for behavioural targeting and the like," he warns. "The government has a powerful role to play in encouraging economic competition. That is one form of regulation – so will all of this work? Will we need more regulation? I think it's too early to say."It's not the only ask Smith has of politicians. In 2017, during a keynote speech at a security conference in San Francisco, he called for a new treaty for cyber warfare. It would build on existing international laws and set out the rules for what is and isn't acceptable online. The agreement was backed by the French President Emmanuel Macron and 51 countries, but there were notable absences on the list of signatories, including the US, China, Russia, India and Brazil.

On why the US refused to sign up, Smith says: "It has come at a time when we have an administration that is less enthusiastic about multilateralism. I think that remains the challenge today. We remain hopeful that there will come a day in the future when the US government will sign." But Smith is encouraged by the United Nations' decision to take up the cause. "If what we do," he says, "leads others to work harder and move faster but use a different name, that's going to be fine."

Tools and Weapons by Brad Smith and Carol Ann Browne, published by Hodder & Stoughton, is out now

Protecting the connected world

Kevin Brown, managing director at BT Security, discusses the steps organisations can take to stay safe in an increasingly digitised world

The modern world revolves around communication – between individuals, between families and between colleagues. At BT we are proud of the role our technology plays in connecting people, and with a network covering 180 countries, we are placing the United Kingdom at the heart of the world's digital economy.

However, technology and our customers' needs are constantly changing. The next generation of networks will need to meet unprecedented challenges, handling exponentially more data than anything that has come before. They'll need to deliver 4K, 8K and later 16k television seamlessly, whilst simultaneously acting as an invisible hub for billions of interconnected devices. They'll also be transporting a hugely diverse range of data – from critical communications for national infrastructure and emergency services, through to the data from your kettle, your car or the sensors your city uses to monitor air pollution. This information will provide actionable insights into almost every aspect of daily life, presenting millions of opportunities to improve communities and build new businesses.

Tomorrow's networks will play a critical role in our society, becoming even more integral to our lives, our businesses and to national success. The opportunities are huge. But so are the challenges. If everything is carried over the network, that network needs to be fast, flexible and built with security at its heart.

To do that, we're leveraging our own world-leading research division, the BT Labs. The same teams who perfected fibreoptics, the technology that underpins all global communications today, are now focused on the challenges of tomorrow.

We are turning that expertise into

BT

IN ASSOCIATION WITH

action, to keep our customers safe in an increasingly dangerous digital world. This year we've launched the world's first commercial grade quantum test network, the foundation for a whole new generation of ultra-secure network technologies.

Our AI-powered cyber defence tools are helping us to identify and even predict threats before they happen, securing our networks against 4,000 attempted cyberattacks every day. And we are developing new technologies that allow our security experts from across the globe to collaborate in real time using fully immersive Virtual Reality Security Operations Centres.

Through our next generation networks, cutting-edge research and world-class security, BT is providing a crucial role in connecting and protecting the networks of the future.

For more information, plase visit: www.bt.com

Q&A
Cyber security principles

How do you keep a global network safe and secure in an increasingly digitised world?

Technology is evolving and so is crime. As such it is important to stay vigilant and work on a strategy of continuous improvement. Cyber resilience – accepting that a breach is a likely eventuality and preparing for it accordingly – has rightly supplanted the traditional understanding of cyber security for many organisations. This is not a defeatist outlook; it is simply a realistic one.

But that's not to say that organisations should simply wait around to be attacked. They should still do everything they can to avoid a breach if possible. Regular and rigorous penetration testing is a good habit to get into. Is the organisation's hardware and software up to date? Are staff well trained and cyber aware?

Artificial intelligence and machine learning are technologies that can be used to automate some aspects of cyber resilience. As the speed of networks and data volumes grow, monitoring processes have to become more automated so that they can ensure the network is running smoothly while human experts concentrate on the more complex actions relating to security. The idea isn't necessarily for AI technologies to replace human insight, but rather to enhance it.

What are the main things that organisations should keep in mind when thinking about security?

Security is never fully solved, and you cannot simply buy your way out of security risk. It is therefore vital that organisations do not become complacent. A "zero trust" mindset – being healthily sceptical of an organisation's security provision while extensively vetting any interaction with external partners is a must-have for businesses in the modern world.

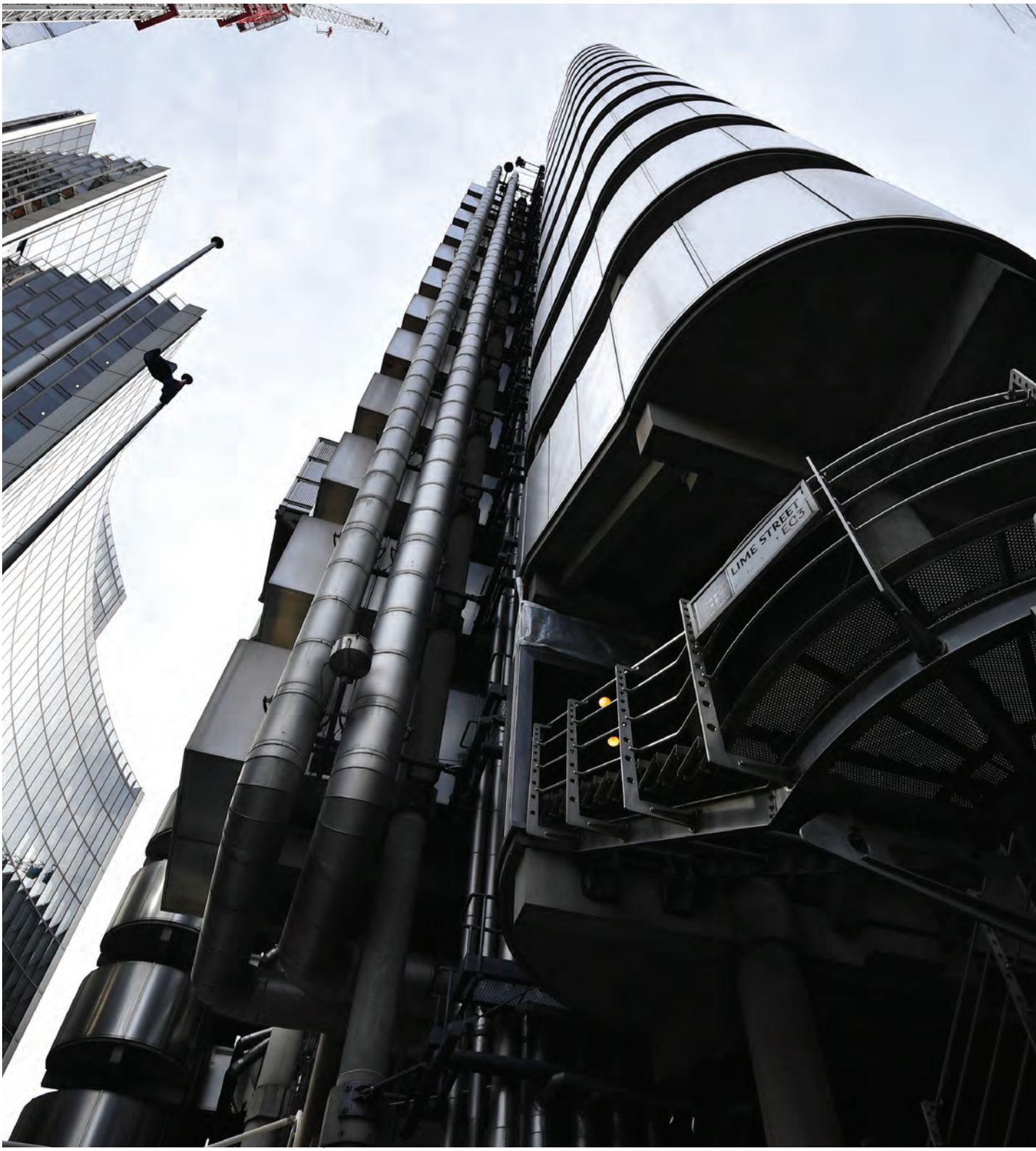
While some organisations may hesitate about committing to the costs of cyber security and resilience provision, it is worth noting that these are tiny compared to the huge costs of recovery that can be incurred in the event of a breach without protection. Cyber resilience is an investment well worth making.

Are you prepared for a worst-case scenario?

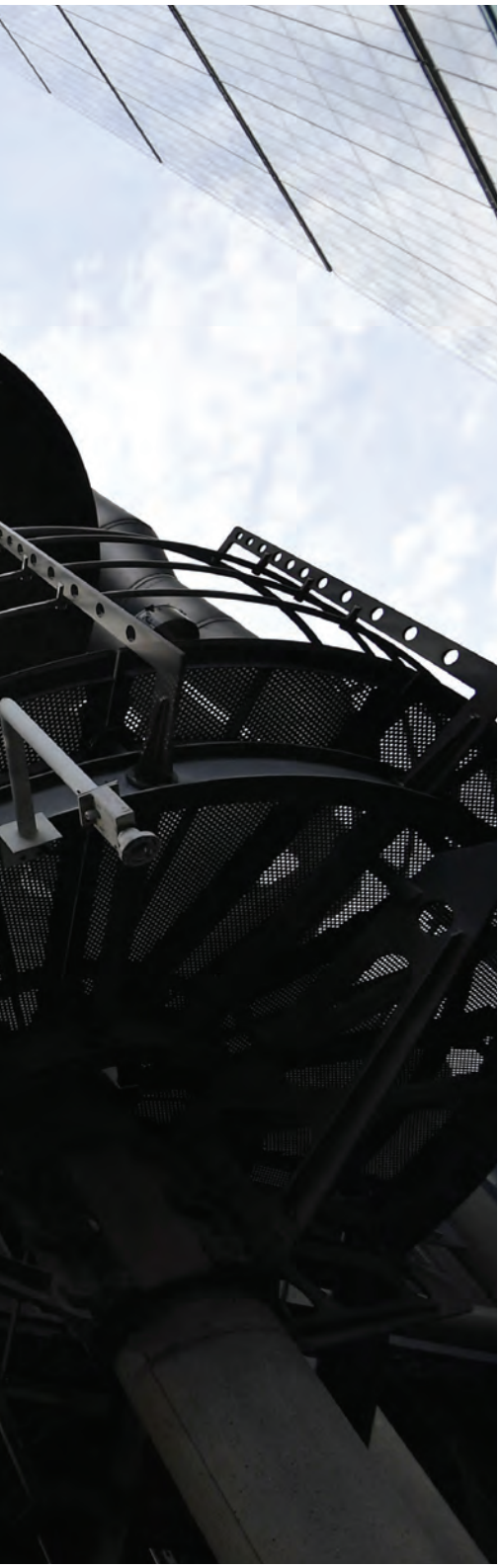
What practical steps can individuals and organisations take to improve their cyber security?

It is important for organisations to understand their assets and priorities. Being able to protect valuable data is not only crucial for the day-to-day operation of a business, but because it has a direct bearing on that organisation's wider reputation.

For all the new technologies, people and behaviours are still often targeted as a major vulnerability in any organisation. Training staff in good cyber hygiene, whether this is something as simple as getting them to change their passwords regularly or being on the lookout for spoof or spam emails, will pay dividends in the long run.



GETTY IMAGES/ BEN STANSALL



The growing industry of paying up

Will Dunn

The first question in the "Ransomware FAQ" page of the Baltimore City website, which answers residents' questions about the cyberattack that paralysed the city's systems for months earlier this year, is: *Why don't we just pay the ransom?*

Baltimore's public services were attacked by Robinhood, a ransomware, which locked files on thousands of computers. The ransom demanded by the hackers was relatively small, at 13 bitcoins – just over $100,000 – but Baltimore was advised by the FBI and security services not to pay. In July, the city approved a $10m budget to recover from the attack.

In June, Lake City, Florida, was also hit by a ransomware attack. Lake City asked the company that provides its cyber insurance to pay the 42-bitcoin ransom – worth just over $400,000 at the time – and was itself liable only for a $10,000 excess payment.

So, why would one city pay a thousand times more than another to rid itself of the same cyberattack? Lake City officials told ProPublica, the non-profit news organisation that has investigated cyber security insurance in detail, that the decision to pay was effectively made for Lake City by its insurer. Baltimore, on the other hand, took the decision to try to recover the files.

ProPublica has found that the Lake City option is increasingly preferred, for obvious reasons, but that it is also feeding two industries: ransomware development, which is accelerating in response to the easy money available from insurers, and cyber insurance, which is growing even more rapidly as businesses and public institutions see others falling prey to ransomware.

Both industries are certainly on the up. The US Conference of Mayors reported 22 major ransomware attacks on cities and public institutions over the first six months of 2019, while KPMG says it expects the cyber insurance sector to grow by 20 to 25 per cent per year for at least five years. By 2025, cyber insurance is widely expected to be a $20bn-a-year industry. While there is no suggestion that reputable insurance companies are doing anything underhand, the growing fear of ransomware is certainly not harming their business model.

This perverse incentivisation may yet backfire, however. ProPublica was told that the FBI found criminals increasingly targeting institutions they know have cyber insurance. And while the amounts currently demanded by hackers are relatively small – Baltimore's new cyber insurance policy has a yearly premium around eight times higher than the original ransom demand – the fact that insurers will pay up will almost certainly lead them to keep demanding more, until insurers no longer pay out. At which point governments and businesses will face the same problem, but it will be much more expensive to fix.

Dr Jessica Barker, co-founder of Cygenta and chair of ClubCISO, talks to Rohan Banerjee about the human side of cyber security

The power of people

Over the past year, nearly a third of UK organisations have suffered from a cyber security breach. Of these incidents, 80 per cent involved phishing, according to a recent poll by DCMS, Ipsos Mori and the University of Portsmouth, with emails often impersonating a senior colleague asking an employee to carry out a special task.

The human side of cyber security, says Dr Jessica Barker, co-founder of digital consultancy firm Cygenta, "stretches far beyond hackers". The way that people interact with technology is a "legitimate social science". And organisations would do well to understand that computers and the tools we install on them for protection are only as effective as people know how to use them.

With an academic background in the humanities and civic design – not a typical mix for a cyber security professional – Barker is perhaps better attuned to these nuances. A self-confessed "people watcher", she is "fascinated" by human behaviour and psychology. "Why do people click on the things that they click on?"

Barker studied politics and sociology at the University of Sheffield, graduating in 2001, before working as a researcher at the Northwest Development Agency. Between 2005 and 2010, she completed a master's programme and PhD in civic design at the University of Liverpool, specialising in place-making and social inclusion. Her research, she explains, explored the impact of technology on people's daily lives. "I was looking at how the internet affected places and organisations… digitisation of services, things like that."

After finishing her PhD, Barker was headhunted by a cyber security startup operating in the defence industry. "At the time, the cyber security conversation was all about firewalls and hackers… there weren't many people looking into the human side of things, to do with people's habits, moods and so on. So they were interested in how they could manage their human resources alongside their technical capabilities."

The move into cyber security has proved enduring and Barker co-founded Cygenta, which "carries out penetration testing and cultural assessments and offers cyber security training for different-sized organisations", with her husband in 2014. Three years later she was named one of the top 20 most influential women in UK cyber security by *SC Magazine*. Since April, she has been chair of ClubCISO, a technology trade body.

Cygenta has worked with clients such as Bupa and several global banks, and, as Barker puts it, aims to "help organisations improve their physical, digital and human security." Physical security, Barker explains, could refer to something "as basic as who has the keys to what…things like fences, cameras and access to control systems." Digital security is "the obvious stuff, like whether an organisation is keeping up to date with its hardware and software." Cygenta's human security brief, meanwhile, focuses on improving "organisational culture".

People can be susceptible to social engineering and spear phishing and fraudulent emails, Barker points out, are becoming more convincing. "There's

CYGENTA

"Cyber security is a legitimate social science"

information out there about us that's publicly available [online] and criminals might track their targets so they can be strategic about what they send over."

Modern phishing emails, she continues, can be designed to "intimidate or even flatter" members of staff. Cyber criminals might impersonate people's bosses in a bid "to have more authority over them." They could use complimentary tactics to cajole them into doing something, such as "telling an employee that they are being hand-picked" for a particular opportunity because they are the most trusted person in the organisation.

Helping employees to become more "vigilant and alert to their inbox" is Cygenta's bread and butter. "We try to show people the triggers they should be looking out for," Barker says, adding that speed is not always the answer. "If people are slower to read through their emails, they can concentrate on what's been said and how it's been said. Maybe they'd see that an email wasn't signed off in the way it was supposed to be."

But to think of cyber security purely in terms of absent-minded employees not reading their emails carefully enough would miss the point. "From an organisational point of view, the more emails people get, you have to accept, the more likely it is that they are going to be a victim [of a spear phishing attack]. The busier you are, the more stressed you are likely to be. So the first step is to think about how you can manage that workflow and reduce stress for people."

Choice of language, Barker highlights, also plays an important role in determining how engaged or aware staff may be when it comes to cyber security. "If you want your employees to be engaged, if you want them to perform well, then you have to think carefully about how you communicate with them. If you focus on the bad things that will happen if they make a mistake, that's less likely to engage them than if you tell them what they can do to protect the organisation, and how important they are in doing that."

What, then, does constitute a good cyber security culture? "Organisations need to have a culture in which people feel comfortable to admit their concerns," Barker says. "The worst kind of security culture is one in which people feel afraid to admit they've clicked on a link. The longer that an incident is left, the more damage it's likely to do ."

When it comes to actual cyber security training, Barker recommends that organisations move away from the traditional, laboured "click and read" approach, with yearly sessions at best. "If you really want to shift behaviour, then there are more interactive solutions. At Cygenta, we organise live hacks. We can come into organisations and show them what happens in the event of a cyber breach. Cyber security can be extremely technical, so we do our very best to demystify it."

For Barker a good cyber security strategy hinges on striking the right "balance" between humans and technology. "You need to make sure that humans are aware of cyber security risks in general," she says, "because that at least gives them a chance of dealing with some of them. But that's not an excuse to not update your software or hardware regularly."

Technology, Barker says, can help make cyber security less of a burden. She recommends password managers [desktop or cloud-based apps that store complex login credentials for multiple accounts], that require people to remember one air-tight password in order to access several, rather than keeping up with the long list that most of us have. What if a password vault gets hacked? "A password manager is [still] less risky than a human trying to remember lots of different 15-character passwords."

Ultimately, Barker says, cyber security is no longer an issue "exclusive to IT departments." As the world becomes more digital, individuals and organisations have a responsibility to adapt to it. The former civic designer quips: "Nowadays, all issues are tech issues, to some degree, aren't they?"

Cyber security is a company-wide priority

James Houghton, chief executive at Phishing Tackle, discusses the importance of people, processes and technology in designing an organisation's digital defences

As technology evolves so too do the risks associated with it. In an increasingly digitised world, where more and more businesses and services have made the move online, it makes sense that crime has followed suit. Cyber security can no longer be thought of as an issue solely for a company's IT department. It requires an organisation-wide strategy which centres on something we in the sector call the "information security triangle". This comprises people, processes and technology.

Indeed, as well as keeping abreast of the latest software and hardware developments, and updating programmes and infrastructure accordingly, it is vital that companies carry out routine checks and penetration tests so that they have an understanding of what constitutes normal system performance. Being aware of this baseline can help organisations to be more alert to any potential indiscretions.

While cyber security is an inarguably very technical field, its human element should not be underestimated. Human beings are the first and last line of a company's defence, and ensuring that they are as cyber aware as possible is an investment that pays for itself in the long term. Too many companies, one might suggest, have adopted a reactive strategy for cyber security. Equipping members of staff with the education and skills needed to spot cyber security problems off the bat is exactly the sort of forward-thinking approach that needs to be established as standard. Making employees more vigilant, sharpening their eyes as to what to look for in fraudulent and phishing emails, not only reduces the potential attack surfaces of an organisation, but, culturally, taking the time to train them, can inculcate a sense of value. Employees that feel trusted and valued are more likely to accept their responsibilities and thrive in an environment that includes and encourages them.

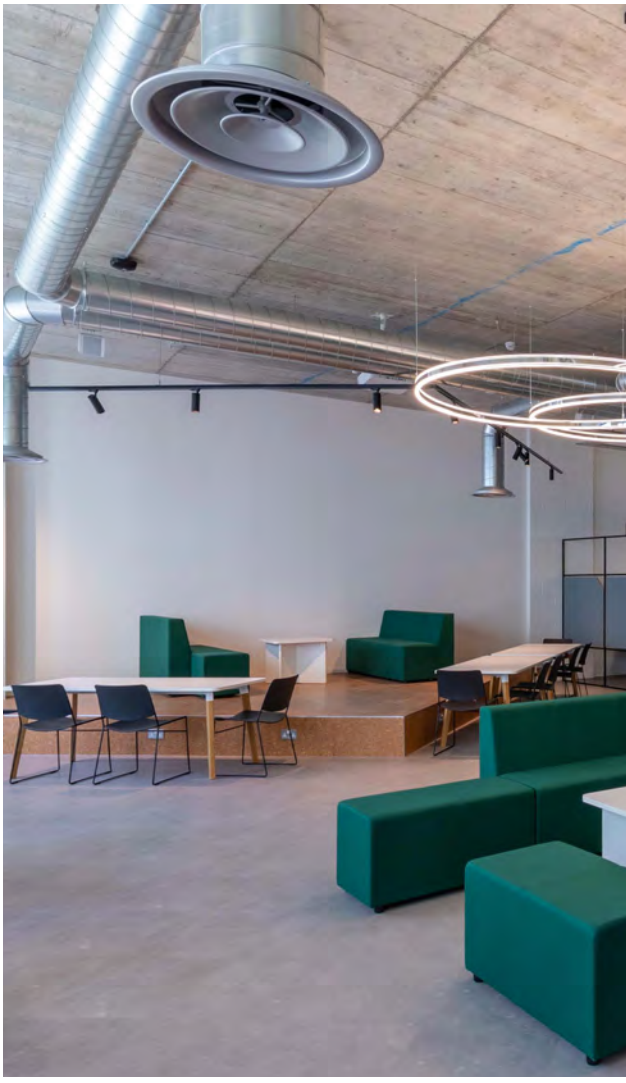
Phishing Tackle, a cloud-based platform that generates simulated phishing emails and malware attacks, helps companies to train their staff by analysing their reactions in response to a variety of challenging cyber security scenarios. The analysis, which is fed back to the companies in real time, allows them to recognise which employees may be more susceptible to an attack. Armed with this information, companies can direct their training and help employees to become better at spotting potential threats. To this end, Phishing Tackle offers a range of interactive quizzes and video tutorials that make cyber security learning more engaging and empowering.

Finger-pointing is not conducive to achieving good cyber security; and organisations that are serious about enhancing their cyber security capabilities should adopt a culture of continuous improvement – one that prioritises the development of their staff while striving to reach the highest standards of cyber hygiene.

Ultimately, when it comes to cyber security, many organisations are still not using the human aspect of their operation to its full capacity. Too often training and education are administered on a reactive basis, rather than being treated as an operational necessity. Ad-hoc training can yield expensive upfront costs, but Phishing Tackle offers a regular, constantly improving and, most importantly, affordable service, used by companies in the public, private and not-for-profit sectors alike.

IN ASSOCIATION WITH

Member of Parliament for Cheltenham Alex Chalk explains how his constituency is playing a key role in shaping the future of UK cyber security strategy



The growth of Silicon Spa

The future belongs to the innovators; and here in Cheltenham, the home of GCHQ, we have found that innovating in cyber security technology can help to underpin our region's future prosperity. With the government stepping in to support a local cyber innovation centre, some of the finest minds from GCHQ are now being deployed to support cutting-edge civilian business startups.

That is generating job opportunities for young people and improving social mobility. It is just the beginning of a larger vision, including a cyber park directly adjacent to GCHQ, which is expected to transform the local economy.

Why cyber security? The internet has made us richer, freer and more connected in ways its founders could never have imagined. But it has also become a vector of espionage, crime and harm. Every British company is a target, and every British network will be attacked – even the NHS, as we know from the WannaCry ransomware campaign. Each attack damages organisations and their users, as well as public trust in our collective ability to keep data safe.

Cybercrime is not something that happens to *other* people. According to the Federation of Small Businesses, 54 per cent of companies polled said they had been a victim of cybercrime in the last year. Accountancy firm Grant

HUB8

HUB8 is a 7,000 square feet co-working space, hosting cyber security startups in Cheltenham

Cheltenham is leading on innovation and expertise

Thornton, meanwhile, reported earlier this year that British businesses lost at least £30bn in the last 12 months alone due to cyber security breaches.

The National Cyber Security Centre is the agency tasked by the government to help make the United Kingdom the safest place to live and work online. It reports to GCHQ and was created as part of a £1.9bn investment in defending national systems and infrastructure, and supporting deterrence of cyber threats. Its mission is to develop a "whole-society capability" where all companies and individuals take the necessary steps to embed cyber security in their business and personal life.

The NCSC supports British business, with its *Small Business Guide: Cyber Security* providing guidance on improving resilience. Its "10 Steps to Cyber Security" guidance is now used by two thirds of FTSE 350 companies, and it is having success. The UK's global share of phishing attacks has dropped from 5.4 per cent in 2016 to below 2 per cent in March 2019. In 2016, Her Majesty's Revenue and Customs was the 16th most-phished brand globally; now, it is 146th, suggesting the UK is becoming a harder target.

But despite that progress, over 130,000 businesses have been affected by cybercrime in the last 12 months. The threat still remains, which is why, even at a time of flat IT budgets overall, total private sector spending on cyber security continues to rise. The UK cyber security market is valued at over £5bn annually, and is increasing fast.

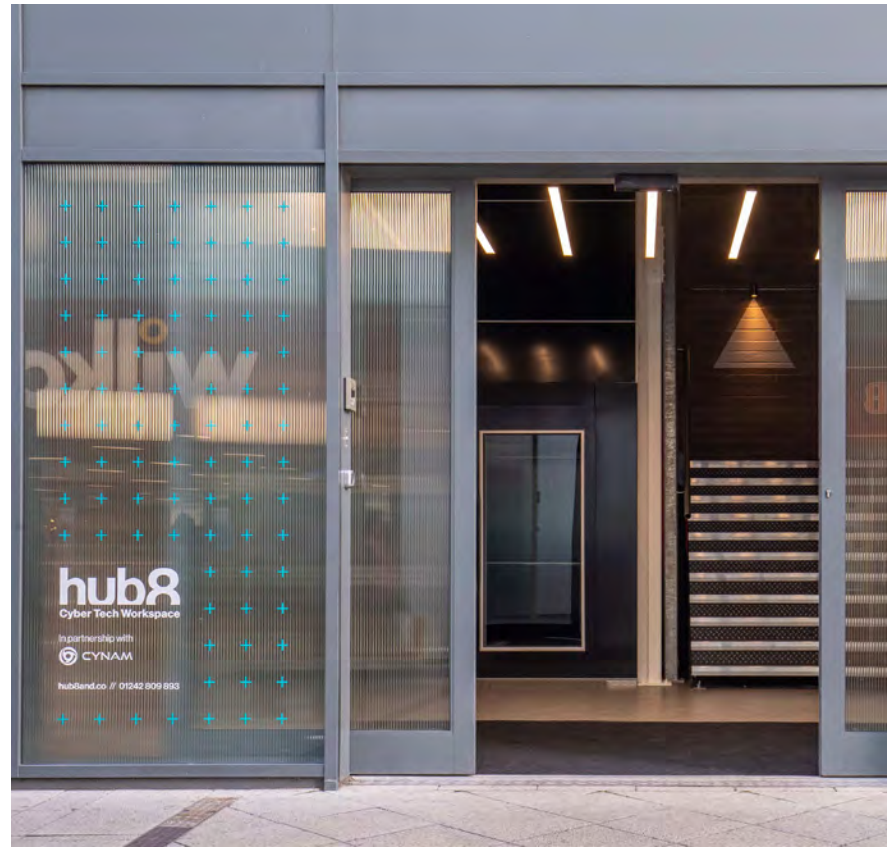
That direction of travel was clear to me back in 2014, when I first set out my vision for Cheltenham to become a national cyber hub. I felt that the opportunity to take advantage of this changing landscape could be harnessed far more effectively.

Although GCHQ was employing some of the most brilliant minds in our country, as a matter of policy they were blocked from applying any of that technical know-how to support civilian startups. Technical excellence was, in effect, going to waste.

Other countries, meanwhile, were taking a far more commercial approach. In Israel, for example, the government had stepped in to build a cyber park directly next to Ben-Gurion University of the Negev to commercialise technologies that had emerged from the security sector.

So, after raising this with the chancellor at the time, George Osborne, in November 2015, the UK government decided to financially support a "cyber innovation centre" in Cheltenham. Since then, this facility has provided an ecosystem in which brilliant minds move in and out of GCHQ, bringing

Investment has catalysed the local cyber economy



the deepest expertise into the private sector and the latest innovation back into government. Several cohorts of startups have already passed through its doors, raising over £35m in investment for their latest security solutions.

That government investment has, in turn, served as catalyst for the local cyber economy. HUB8, for example — a play on Bletchley Park's Hut 8 — is a new co-working space in the centre of Cheltenham which launched earlier this year, hosting numerous digital startups in the area. Furthermore, Gloucestershire College is now offering cyber degrees accredited by GCHQ in collaboration with the University of the West of England in Bristol.

Future plans are no less ambitious. The government has committed £23m to help Cheltenham develop a cyber park adjacent to GCHQ. This 45-hectare site will become a magnet for the many local businesses currently scattered around the region that operate in the cyber security sector. And the range of expertise on offer in Gloucestershire is very impressive. Only recently I met a team of Microsoft experts based in an ordinary office block in Cheltenham who devised the patch to a vulnerability in Internet Explorer thereby protecting hundreds of millions of people all over the world.

Plans for Cheltenham's cyber park are advanced, with road improvement works in line to start in the early part of next year. I am pressing for businesses to get on site as soon as possible thereafter.

It is an unfortunate reality that cybercrime is here to stay. "Off the shelf" tools mean that less technically savvy criminals are now better equipped than ever to extort, steal and blackmail. And criminals are becoming increasingly aware of the rich pickings on offer. But with government support, I am pleased that Cheltenham will be playing an ever greater role in fighting back.

Bring your own device, not your problems

Allowing employees to use their own devices in the workplace can introduce new security risks, warns Robert Allen, director of marketing and technical services at Kingston Technology

Flexibility is the ongoing trend of the 21st century working environment. In many cases, bring your own device (BYOD) is an integral part of the conversation. It improves productivity, allows companies to omit requirements on fixed hours, and can remove the significant expense of office space and equipment. But there are also problems when it comes to using personal devices for work purposes. If unencrypted devices are lost or stolen, third parties have potential access to confidential data, resulting in dire effects for an organisation, threatening its reputation and finances, in part due to the EU's GDPR legislation.

So, how do you reap the benefits of BYOD, while ensuring the integrity of your data security? The answer lies in education, strict security policies and hardware encryption. There is still a long-standing variable within the human element/insider threat factor, which contains the issues of lax standards and policies, along with lack of accountability and responsibility. Data, personal identifiable information and confidential information are still the key elements in need of our most profound protection.

Recent breaches, exposures and compromised assets have highlighted that most of these incidents were from preventable mistakes that we allowed to happen. Simple oversights ranging from lack of attention, prioritisation of proper standard and policies and procedures in place were the culprits in the majority of incidents.

How secure your data is depends on the kind of encryption you use. Knowing the differences between them should affect your IT policy. Careful planning and adequate training ensures employees are still able to bring their own devices to work, while sensitive company data remains protected. Beyond SaaS and software encryption, employees may need to store data on local devices. How do you mitigate risks in this scenario? Hardware-encrypted solid state drives (SSDs) provide end-to-end data protection. It's essential that anyone working remotely with a laptop equip themselves with SSDs that are hardware-encrypted. There is a whole host of features to protect BYOD and mobile users, such as leveraging data loss prevention (DLP) software suites with compatible self-encrypting drive SSDs or TCG Opal 2.0, to Bitlocker hardware-encrypted solutions such as eDrive.

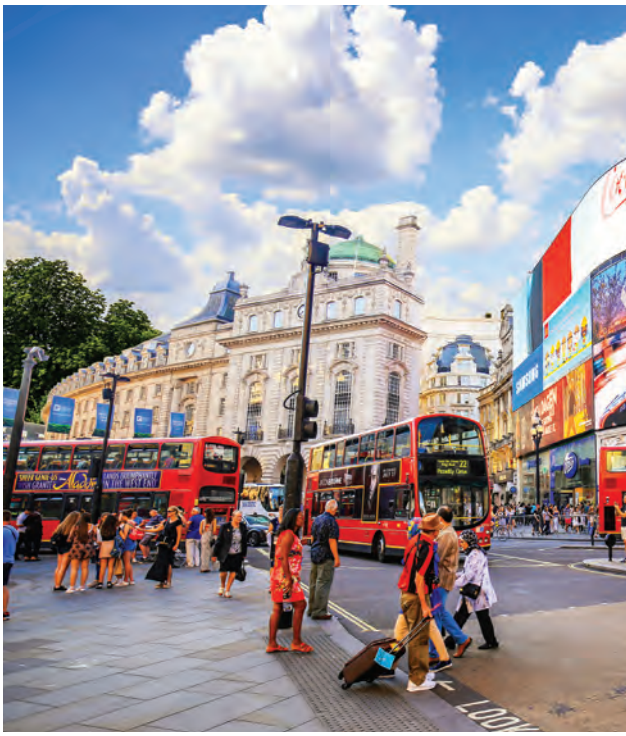
I always challenge companies that present or pitch at our offices about the devices they are using and I am shocked at how many have overlooked using a hardware-encrypted SSD. When you need portability, USB drives are an essential tool for data transport and backup. But while their size offers mobility, it does also make them easy to lose. For a small price, hardware-based encryption built into external USB devices mitigates this risk. The top-of-the-line Advanced Encryption Standard (AES) 256-bit used in high-end encrypted USB drives is secure enough to be FIPS-certified, endorsed by government organisations.

Agreeing to BYOD requests may seem like an inexpensive and simple way to create a relaxed working environment. But without taking a few precautions, the potential risks to company data security could prove costly. Enforcing a solid hardware encryption policy allows you to embrace the BYOD culture without adding risk, cost and expensive tools.

For more information, please visit: kings.tn/BYOD

New research shared exclusively with *Spotlight* reveals how hackers launched nearly 1,600 fake WiFi networks in central London to spy on the public. Oscar Williams investigates

The weaponisation of WiFi



In October 2017, it emerged that suspected Russian agents had launched an unconventional intelligence operation in Europe. The agents equipped a small fleet of drones with WiFi routers, and then flew them to NATO bases in Poland and Estonia. As the aircraft approached the military compounds, soldiers' smartphones began connecting to the WiFi.

According to the *Wall Street Journal*, the Russian agents exploited these connections to compromise devices, identify troop numbers and steal sensitive personal information that could later be used in intimidation campaigns. NATO described the incident at the time as an example of the "hybrid challenge" allied troops were facing.

The weaponisation of WiFi is not confined to the military, however. In major global cities, bogus WiFi networks have quietly become prized assets for cyber criminals. New research shared exclusively with *Spotlight* reveals that, between August 2018 and August 2019, nearly 1,600 fraudulent WiFi networks were in operation across central London, imitating familiar brands such as O2, BT and Hyatt.

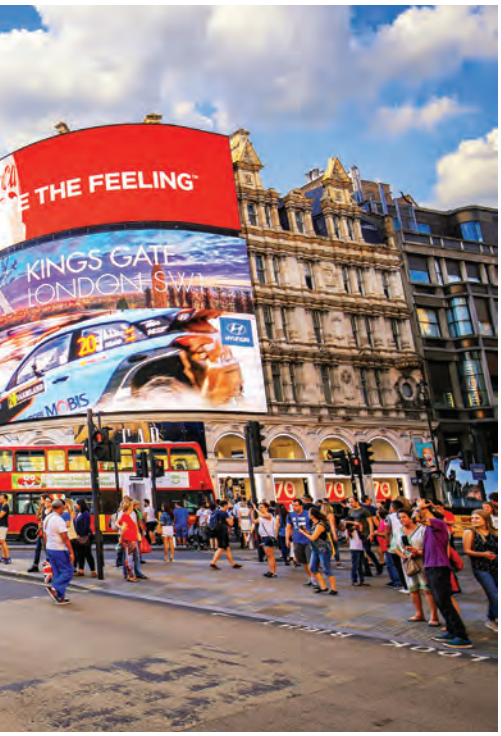
Zimperium, the mobile security provider which produced the research, blocked 5,561 attacks over the course of the year. But given that only a small percentage of phones would have been running Zimperium's software in the studied area, it's possible that tens of thousands more attacks would have gone undetected, exposing users' data and potentially leaving their devices vulnerable to further surveillance.

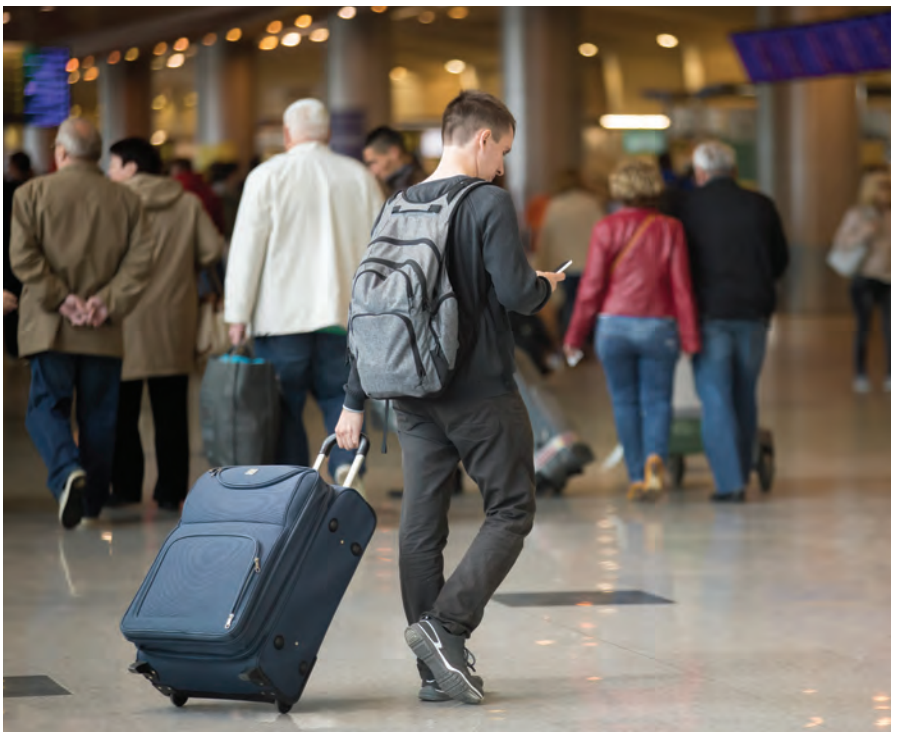
So-called "man in the middle attacks" exploit a fundamental flaw in the way mobile devices operate. "The dumbest part of smartphones is the phone introduces itself to the network, not the other way around," explains Zimperium's JT Keating. "So the phone literally goes through every network it's ever connected to and says: 'Hey are you Starbucks? Hey are you Google? Hey are your Marriott?' All it takes is for the network to go, 'well yes I am,' and then it connects."

Owning a network offers an unparalleled vantage point for hackers. It enables them to watch the traffic that passes through and "see what passwords float by", says Keating. "If you control the network, you control the encryption. But the ultimate objective is to be persistent on the device."

With unfettered access to a smartphone, there is little a hacker could not find out about its owner. But how do they maintain access to a device once it has left the WiFi network? There are two common ways in. The network may send users to a fake version of a popular website and use it to deliver malicious code without your knowledge. Alternatively, hackers can deliver security exploits through the "captive portal" - the page you see when you sign into a new WiFi network. Simply agreeing to the terms and conditions may be enough to deliver an attack.

SHUTTERSTOCK/FIZKES





For sophisticated hackers, breaching a personal device is often just the first part of a grander plan. If a phone has been breached, a user who returns to their office and logs into the work WiFi may compromise the integrity of the entire corporate network. It is, says Keating, "the easiest way" to target an organisation.

Most of the attacks in London took place around major tourist spots. Zimperium's analysis shows that it thwarted a high number of attacks in Soho, Mayfair and Fitzrovia. There were also a considerable number in the City and Westminster. "What we see in cities like London is significant concentrations around government buildings and [...] significant concentrations around tourist environments," says Keating.

Owning a network gives hackers an advantage

On the streets surrounding the Palace of Westminster and Parliament Square, at least 15 "critical attacks" were blocked by Zimperium's software, which is typically used by government agencies and major businesses. While this suggests that a number of fraudulent networks had been established in the area, the analysis does not show the number of attacks on phones which were not protected by mobile security software and may have been successfully compromised.

In 2016, reportedly Russian hackers breached the personal email account of John Podesta, a senior member of the US Democratic National Committee, exposing thousands of messages. A year later, a cyberattack was launched on the Palace of Westminster, with hackers attempting to infiltrate MPs' emails. In the wake of the attacks, cyber security has become a hot topic in our politics.

The National Cyber Security Centre (NCSC), launched in 2016 to improve the UK's cyber defences, meets with politicians from all parties in Westminster every quarter as part of its work to protect British democracy. In late October its director, Ciaran Martin, warned that "too many basic attacks" in the UK are still succeeding. "There are too many incidents causing too much harm."

The NCSC says that one of the simplest ways individuals can protect themselves is to ensure that their phones are constantly updated with the latest software. Members of the public and politicians alike would do well to follow the advice. After all, as Zimperium's research shows, it isn't just NATO troops who are finding themselves in the cross-hairs of hackers.

True cyber resilience requires a coordinated response from the public and private sector, writes Minister of State for Security Brandon Lewis

What is the government doing to keep the UK safe?

From smartphones and social media, to online shopping and banking, the advent of the digital age has made our lives easier at work and at home, and brought us closer together in a multitude of ways.

But advances in technology have also brought with them new challenges, because the technology that has transformed the way we live can also be turned against us.

It has given criminals and hostile states the opportunity to try to interfere with our national infrastructure, attack our businesses and steal personal data more easily and quickly, and from anywhere in the world. The National Crime Agency (NCA) estimates that cybercrime costs the United Kingdom billions of pounds every year.

We've all seen the headlines: the cyberattack against British Airways in 2018 that saw hundreds of thousands of its customers' data compromised, breaches affecting Eurostar, Dixons, Carphone Warehouse and Ticketmaster. The WannaCry ransomware was one of the largest and most disruptive attacks that the UK has faced, hitting the public and private sector alike, and affecting the vital work of the National Health Service. We have subsequently linked the attack to a group in North Korea, known as the Lazarus Group, which has been responsible for a range of cyberattacks across the globe.

As the minister of state for security, I am clear that we must use all the levers at our disposal to tackle cybercriminals head on. The government is committed to safeguarding our digital information, data and networks at home and abroad. Our Five Eyes partnership with Australia, Canada, New Zealand and the United States is vital to this work. This year's five-country ministerial

SHUTTERSTOCK/TT STUDIO

Crime is changing and we must keep pace with it

meeting saw representatives discuss the common risks posed by new technologies, and we agreed to continue to develop and share learning on these evolving threats to improve the collective response.

We are also working closely with operational partners and European Union member states to prepare for our departure from the bloc. After Brexit, we will continue to work together with our European partners to promote cooperation and stability in cyberspace. The UK is, and will continue to be, one of the safest countries in the world.

Collaborative work is crucial, not just because cybercrime threatens our national security but because being the victim of a hack can be frightening, embarrassing and costly. Both individuals and organisations can be caught up in these incidents. Around a third of all UK businesses and one in five charities reported having cyber security breaches or attacks in the last 12 months.

Our five-year National Cyber Security Strategy, launched in 2016, brings together the best from government and industry to strengthen our defences and fight criminals. It is backed by £1.9bn worth of investment. The National Cyber Security Centre (NCSC), NCA and police are at the heart of this strategy. Together, they form a world-leading cyber security team for the UK which has given advice, coordinated the government response, and provided reassurance in relation to in excess of 1,800 incidents.

One example is an email scam last year where criminals tried to send more than 200,000 emails purporting to be from a UK airport and using a non-existent gov.uk address to try and defraud people. These emails never reached the intended recipients thanks to the NCSC's world-leading Active Cyber Defence system, which detected the suspicious domain name, meaning the recipient's mail providers never delivered the fraudulent messages.

Building the resilience of businesses and individuals to this type of crime and ensuring law enforcement agencies have the capabilities they need to tackle it, are also important aspects of our updated Serious and Organised Crime Strategy, published last November. The NCA leads the law enforcement response to cybercrime, coordinating investigations across dedicated teams in every police force in England and Wales. This approach is vital to preventing this type of crime, pursuing the perpetrators and protecting victims. Driving up arrests and convictions will help to deter potential criminals, and we are determined to ensure there is no safe space for them to operate in.

An example of this valuable work is the NCA's investigation into 24-year-old Zain Qaiser, a prolific cybercriminal who targeted millions of computers with ransomware in an internet blackmail campaign. Investigators identified that he received more than £700,000 through multiple bank accounts – although the total is likely to have been much higher. He was brought to justice following a complex investigation by the NCA, in conjunction with international partners, and jailed for more than six years in April.

An NCA-led Prevent programme has been designed to divert talented young people away from cybercrimes like these and into lucrative roles in the tech sector. The Home Office, meanwhile, funds officers at the national, regional and local tiers of law enforcement. This means that in every one of the 43 force areas there is someone dedicated to helping businesses and individuals guard themselves online.

But there is more that needs to be done. Crime is changing, and we must evolve to keep pace with it. Businesses have a responsibility to protect themselves and their customers, as most attacks could be prevented by adopting simple security measures. And every citizen must also play their part. Advice and guidance are available from the NCSC and Cyber Aware, the government programme to help individuals and smaller organisations protect themselves online, which is kicking off a fresh campaign this autumn.

INSIGHT

The state of UK cyber security

The Cyber Security Breaches Survey 2019 gives an overview of the scale and nature of cyberattacks affecting UK organisations

27%

Around a third of UK businesses and charities have experienced a cyberattack in the past 12 months, down from 43 per cent in 2017-18

80%

Most cyberattacks affecting businesses and charities were phishing-related, with almost one in three of those involving hackers impersonating a senior member of an organisation's staff over email

28%

The percentage of businesses and charities sending staff on a cyber security training courses has increased 10 per cent on the previous year

49%

Nearly half of all UK businesses have introduced all of the technical controls listed under the NCSC's Cyber Essentials programme

SHUTTERSTOCK/DESIGN BY LEON PARKS

£12,050

The average cost to UK businesses that experienced a cyber breach over 2018-19 was slightly higher than the average cost incurred by similarly afflicted charities in the same period – £9,470

1/3

Around a third of UK businesses and charities have introduced written cyber security guidelines for employees in the past 12 months

1/5

Roughly one in five UK businesses and charities affected by a cyberattack said that the incident caused a negative outcome, such as the loss of data or assets

SOURCE: DCMS, UNIVERSITY OF PORTSMOUTH AND IPSOS MORI

CYBER SECURITY

The latest contracts, jobs and training

THESE CONTRACTS ARE NOW OPEN FOR TENDERS

1. Department for International Trade
Penetration testing services
Bid deadline: 13th November
Tender value: £100,000
The Department for International Trade is interested in working with ethical hackers and security consultants to test its digital defence capabilities.
Contact: DITcommercialenquiries@trade.gov.uk

2. Ministry of Defence
DE&S enterprise and risk management tool
Bid deadline: 30th November
Tender value: £10m
The MoD is looking for a cyber security partner to carry out risk assessments and staff training programmes in its offices and on sites based in the South West.
Contact: ryan.miller731@mod.gov.uk

3. Ministry of Defence
Provision of defence cyber protection tool
Bid deadline: 27th July 2020
Tender value: £10m
The MoD is seeking a cyber security partner to design and maintain military-specific software packages to be used in its offices and outposts across the country as part of a three-year contract.
Contact: isscomrclgroup@mod.gov.uk

Total value: £20.1m

Tender and framework data supplied by

tussell

THE LARGEST CONTRACTS OPEN FOR BIDS SOON

"Pre-Information Notices" give advance warning of contracts that will soon be open for tenders.

1. Cabinet Office
Cyber security services 3
The Crown Commercial Service, as the authority on this brief, intends to put a pan-government collaborative agreement for the provision of cyber security services and training to be used by all central government departments and public sector bodies.
Contract value: £100m

2. National Police Chiefs' Council
Digital forensic services
The NPCC, as part of its Transforming Forensics Programme and acting through Dorset Police as their testbed, will look for a cyber security partner to help enhance existing and deliver new technologies relating to cyber security.
Contract value: £20m

3. Wrexham County Borough Council
WCBC firewall
WCBC will be looking for a new cyber security partner to construct its new firewall in order to protect the region's valuable data relating to finance, assets and its citizens.
Contract value: £600,000

Total value: £126.6m

CYBER SECURITY JOBS NOW OPEN FOR APPLICATIONS

Head of Information Security, Department for Education
Salary: £60,290
Location: Various (London, Coventry, Manchester and Sheffield)
Closing date: 3rd November
The DfE seeks an experienced cyber security professional to implement and oversee the rollout of new defensive hardware and software. They will liaise with employees at all levels of the organisation, giving them clear guidance on good cyber hygiene.

Senior Lecturer in Cyber Security or Digital Forensics, Northumbria University
Salary: £35,844-£51,034
Location: Newcastle
Closing date: 3rd November
Northumbria University wants to recruit an experienced academic to contribute to its research into AI, data science and machine learning methods of cyber security and digital forensics, while also teaching on undergraduate courses.

Cyber Security Lead Accreditor, Ministry of Defence
Salary: £38,623
Location: Wyton
Closing date: 10th November
The MoD is looking to appoint an independent assessor of its cyber security risks. The role will involve auditing various military and government technologies and delivering risk assessment analysis.

Senior Lecturer and Research Associate in Cyber Security, De Montfort University
Salary: £39,152-£51,034
Location: Leicester
Closing date: 18th November
De Montfort's Faculty of Technology seeks an expert in digital forensics and cyber threat intelligence to contribute to its research on network and cloud security and penetration testing, with a focus on systems used in industrial control systems for factories.

G6 Head of Cyber Consultancy and Design Service, Home Office
Salary: £64,736-£74,446
Location: London
Closing date: 29th November
The Home Office is looking to hire a senior cyber security architect, responsible for the secure design of its central computer systems and data stores. They will create and constantly review government IT infrastructure.

Head of Corporate Reputation and Crisis Management, Visa
Salary: Competitive
Location: London
Visa wants to recruit an experienced public relations professional, with a technology background and solid legal understanding, to oversee its advance crisis strategy in any event of a cyber security breach or service disruption.

CYBER SECURITY EDUCATION AND TRAINING OPPORTUNITIES

MSc Cyber Security, University of York
This taught, one-year postgraduate course, accredited by the NCSC, covers the breadth of cyber security essentials for workplace environments, including firewalls, malware detection, cryptography, improving employee awareness, and reputation management in the event of a breach.

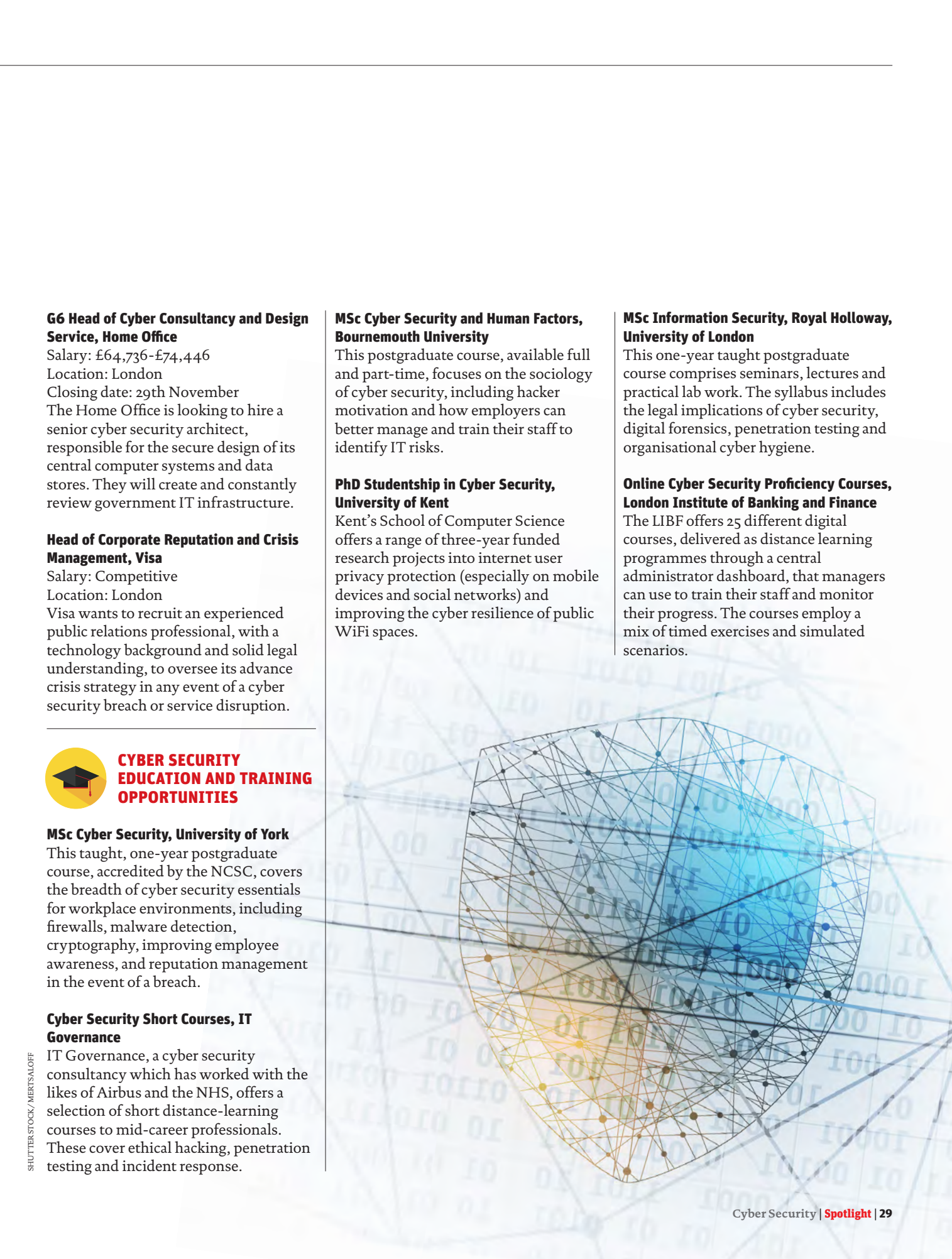
Cyber Security Short Courses, IT Governance
IT Governance, a cyber security consultancy which has worked with the likes of Airbus and the NHS, offers a selection of short distance-learning courses to mid-career professionals. These cover ethical hacking, penetration testing and incident response.

MSc Cyber Security and Human Factors, Bournemouth University
This postgraduate course, available full and part-time, focuses on the sociology of cyber security, including hacker motivation and how employers can better manage and train their staff to identify IT risks.

PhD Studentship in Cyber Security, University of Kent
Kent's School of Computer Science offers a range of three-year funded research projects into internet user privacy protection (especially on mobile devices and social networks) and improving the cyber resilience of public WiFi spaces.

MSc Information Security, Royal Holloway, University of London
This one-year taught postgraduate course comprises seminars, lectures and practical lab work. The syllabus includes the legal implications of cyber security, digital forensics, penetration testing and organisational cyber hygiene.

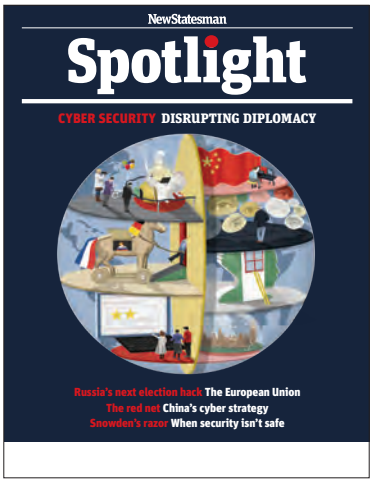
Online Cyber Security Proficiency Courses, London Institute of Banking and Finance
The LIBF offers 25 different digital courses, delivered as distance learning programmes through a central administrator dashboard, that managers can use to train their staff and monitor their progress. The courses employ a mix of timed exercises and simulated scenarios.

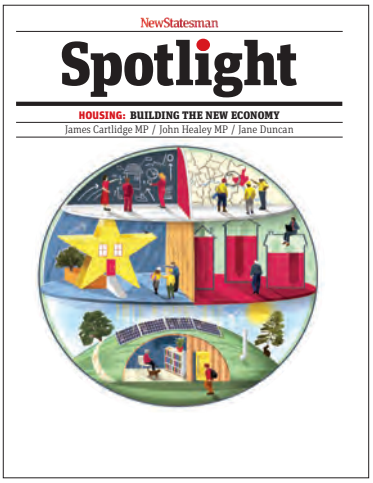


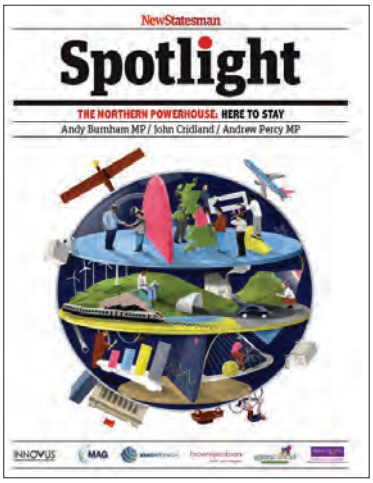
SHUTTERSTOCK / MERTSALOFF

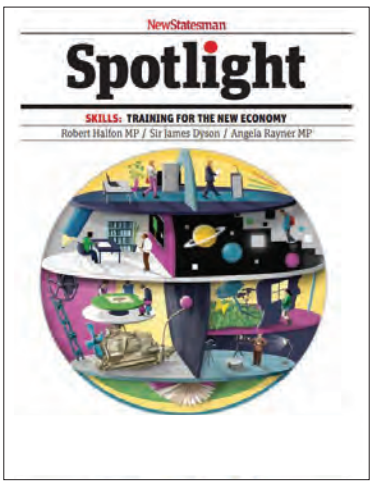
NewStatesman

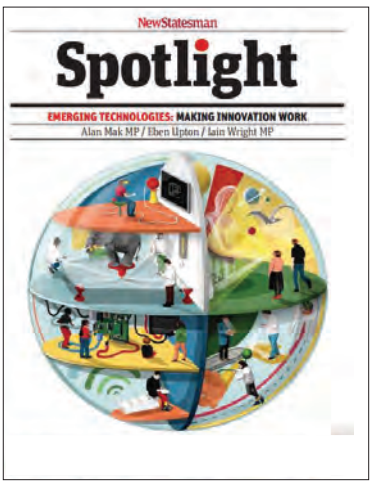
Spotlight

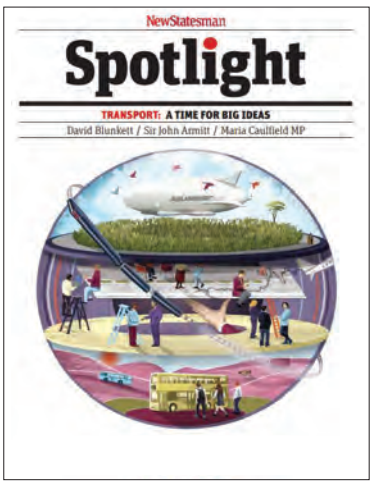












Read more in-depth interviews and features and download full policy reports at:

newstatesman.com/spotlight

US Huawei ban is more about trade than cyber security

At the end of 2018, the US passed a bill preventing the federal government and its agencies from doing business with the Chinese technology giant, Huawei. In 2019, the company, along with several dozen subsidiaries and affiliates, was added to the US's "entity list", severely restricting US companies' ability to do business with one of the world's largest telecommunications equipment firms. In response, American tech companies severed their links to the multinational, including Microsoft, Google and Intel.

"It's a national security concern," US President Donald Trump told reporters last month. "Huawei is a big concern of our military, our intelligence agencies, and we are not doing business with Huawei." The "concern" Trump had was over the ability of the Chinese corporation – with ties to the Chinese Communist Party and People's Liberation Army – to use its control over telecommunications infrastructure to intercept data from individuals, corporations and government. As well as potentially facilitating intellectual property theft and cyber espionage, Chinese integration into Western projects for new critical national cyber infrastructure would give China the upper hand in any potential cyber war.

But Trump also revealed something else in the same press conference: "We're not doing business with Huawei. We're going to do our own business. You know the old fashioned way? We'll do it right from within the United States, which is what I've been saying for a long time… Speaking of tariffs, there are no tariffs if you want to build or make these products in the United States. There are no tariffs whatsoever." The new restrictions on Huawei products did not involve tariffs on their import, but instead restricted them regardless of where they were made. The laws did, however, coincide with the trade war between the US and its new superpower rival in the East.

Despite the rhetoric, the anti-China ban has more to do with economic concerns than fears of espionage, writes Jonny Ball

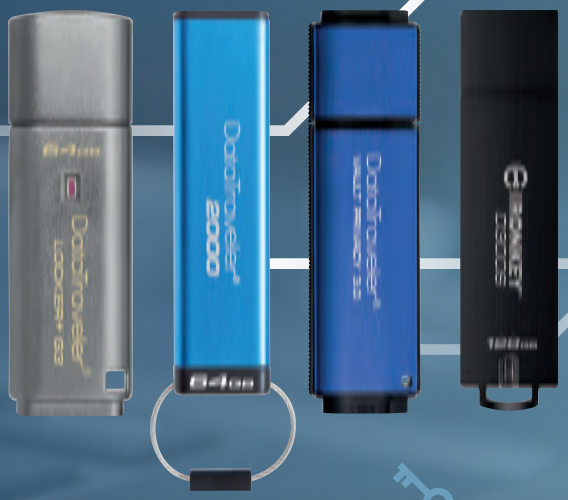
Were the moves against Huawei about preventing a major threat to the nation's cyber security, and maintaining advantage in a future cyber war? Or were they about Trumpian efforts to reshore manufacturing jobs back to the United States? "Huawei is something that's very dangerous…from a security standpoint, from a military standpoint it's very dangerous," he told reporters in May, before telling them that it was possible that Huawei "would be included in some kind of a trade deal". His commitment to anti-Huawei measures has ebbed as negotiations with the People's Republic have progressed, suggesting that the company is less a cyber security concern, and more a pawn in a continuing trade war.

Huawei's phone sales continue to rise whilst Apple's market share falls, and it now sells the second most mobile units after Samsung. Trump's efforts to "make America great again" depend partly on stemming China's inexorable rise. Ironically, his efforts to do so might actually result in the opposite. Restricting Huawei's access to American goods could act as the catalyst for China to accelerate its own production of high technology, and move away from its former role as the world's factory for cheap, low-quality goods. The Communist Party's "Made in China 2025" plan intends to do just that.

Kingston TECHNOLOGY

Data security solutions for BYOD

Encrypted USB sticks and SSDs



#KingstonIsEverywhere

For more information, please visit
kings.tn/BYOD